Applications of Group Theory

Applications of Group Theory

Dongxian Tang[1, †], Zichang Wang[2, *, †], Bangning Yue[3, †]

[1]Faculty of Science, McMaster University, Hamilton, Ontario, L8S4L8, Canada

[2]Leicester International Institution, Dalian University of Technology, Panjin, Liaoning 110000, China

[3]Hurtwood house, Dorking, Guildford, RH5 6NU, United Kingdom

[*]zw173@student.le.ac.uk

[†]These authors contributed equally.

Abstract. Groups play a fundamental role in Abstract Algebra: many algebraic structures, including rings, fields, and modules, can be seen as formed by adding new operations and axioms based on groups. Researchers often use group theory to explain many kinds of phenomena. In recent years, group theory has been introduced into crystallography to further explore the macroscopic symmetry of crystals from a mathematical point of view. In this paper, the applications of group theory in crystallography and magic cubic will be discussed. Basic definitions and models of these fields are demonstrated. A finite group is a group with a finite number of elements, which are the important contents of group theory. Besides, this paper proves that $n-1$ elements in a n order group can completely decide the n^{th} element and gives a method of the n^{th} element in a commutative group of order n. The analysis suggests that the research method of group theory has an important influence on other subjects.

1. Introduction

In the 19th century, Galois founded group theory and used it to solve the problem of the quintic equation. In the past two hundred years, group theory has penetrated geometry, algebraic topology, function theory, functional analysis, and many other branches of mathematics. It has important applications in theoretical physics [1], quantum chemistry, algebraic coding, automata theory, and so on. Particularly, crystallography needs to figure out the mathematical model of crystal structure by group theory. An ordered group has at least one generator, and it is viable that a group has more identified elements than the amounts of generators for everyday applications [2].

Pain presented sum rules for Clebsch–Gordan coefficients in the framework of SO(4) group-theoretical description of the hydrogen atom. The main results are obtained using properties of the Runge-Lenz-Pauli vector, in particular expressing the matrix elements of the powers of its last component both in spherical and parabolic basis. Connections with the Stark effect and diamagnetism of the hydrogen atom are outlined [3].

Nieto proved that it is not always true, since they do not have a version of Lagrange's theorem for generalized groups. Also, they proposed Slow-type theorems for generalized groups [4]. Liu proposed a renormalization group (RG) theory of Eigen microstates, which are introduced in the statistical ensemble composed of microstates which are obtained from experiments or computer simulations. This theory can be used in research of critical phenomena both in equilibrium and non-equilibrium systems without considering the Hamiltonian, which is the foundation of Wilson's RG theory and is

absent for most complex systems [5]. Abruzzi uncovered 2-group symmetries in 6d superconformal field theories. These symmetries arise when the discrete 1-form symmetry and continuous flavor symmetry group of a theory mix with each other. This paper also discussed a mixed Hooft anomaly between discrete 0-form and 1-form symmetries in [6]. Debnath focused on the paper, which introduced a neutrosophic fuzzy soft set (NFSS) to deal with uncertainty parametrically, and it gives the approximate solution to the problem. Then the authors proposed an algorithmic approach for group decision-making (GDM) problems using a neutrosophic fuzzy soft matrix (NFSM) and its related properties [7]. In Tomas's paper, the principle of mathematical induction was enunciated as a method of proof of formal propositions. In recent theoretical work on the multiple-slit experiment, people used this way to prove two important theorems—the generalized hyperbola and hyperboloid [8].

This essay devotes to summarizing some basic applications of Group theory, especially those which is connected to crystallography and the properties of magic cubic. Models of these fields are discussed, and the fundamental applications of group theory on these objects are demonstrated.

2. Crystallography

In this section, we will talk about the application of group theory in crystallography.

A group is a collection of elements that are interconnected according to some laws and is a collection of elements with specific properties and interconnections.

It is a collection of elements of a class with specific properties and interconnections. The elements of a group can be letters, numbers, and symmetry operations.

In crystallography, the elements of point groups and space groups are symmetry operations. The group can be expressed as:

$$\mathrm{G} = \{\mathrm{A}_1, \mathrm{A}_2, \mathrm{A}_3, \mathrm{A}_4, \cdots \mathrm{A}_\mathrm{N},\} \quad (1)$$

$A1, A2, A3, A4, \ldots, An$ are called the elements of the group. n is called the order of the group, i.e., the number of elements.

N is the order of the group, i.e., the number of elements. It can be either an infinite set or a finite set like the point group and space group in crystallography.

However, this set G must satisfy the following four rules to be called a group.

Definition 2.1. Closeness

The product of any two elements of a group or any square is still an element of the group. It is called the closure of a group.

We can use $A \in G, B \in G$ to denote that both A and B are an element of the group G. If $AB = C$, then C are still an element of the group G, denoted as $C \in G$. If $A^2 = D$ or $B^2 = F$, then D and F are still elements of the group G, denoted as $D, F \in G$. However, it should be noted that AB is not necessarily equal to BA, and the exchange law in group theory is not universal.

Definition 2.2. Unit elements (constant elements)

There must be a unit element E in the group G. E means that each element of the group can be permuted with its pair and make them invariant. That is, $AE = EA = A$, $BE = EB = B$, E is called the unit element or constant element (equivalent to the primary axis of symmetry in the point group).

Definition 2.3 The multiplicative law of union

The elements of group G all obey the multiplicative law of union, i.e., A, B, and C are all elements of the same group. Then, $(AB)C = A(BC) = ABC$.

Definition 2.4. Inverse elements

Each element of group G must have an inverse element, which is also an element of the group. The inverse element of A is denoted by A^{-1}. Then, $AA^{-1} = A^{-1}A = E$. Any set of elements that has the above four basic properties constitute a group.

The point groups or space groups in crystallography are consistent with the properties of groups and satisfy the above rules.

Groups can be divided into finite groups and infinite groups. Point groups and space groups in crystallography are both finite groups; that is, the number of elements in a group is finite. Matrix representation of symmetry operations.

If the symmetric elements are placed in a right-angle coordinate system, the three-dimensional coordinates x, y, z of vector r can be transformed into x_1, y_1, z_1 by the symmetry operation.

This transformation of vector coordinates is called symmetric transformation. The coordinates of this symmetric transformation can be represented by a matrix. Therefore, the matrix representation of the symmetric operation

Therefore, the matrix representation of symmetric operations is to describe the coordinate transformation of the vector r before and after the symmetric operation in matrix form.

The various symmetric operations are represented in matrix form below.

(1) $I(L1)$ matrix representation

It is called the primary axis of symmetry, which is also called the constant operation or the all-same operation in group theory.

For example, the new coordinates x_1, y_1, z_1 are the same as the initial coordinates after the operation. The operation can be expressed as a unit square: $\begin{vmatrix} x_1 \\ y_1 \\ z_1 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix} \begin{vmatrix} x \\ y \\ z \end{vmatrix}$.

(2) Matrix representation of the symmetry plane (σ)

The symmetry operation of the symmetry plane is a reflection, the result of which is that the coordinates of both sides of the symmetry plane are the same, but the signs are different.

When the plane of symmetry is consistent with the three main planes xy, xz, and yz in the right-angle coordinate system, then a vector under the action of the plane of symmetry, its reflection results in a change of sign perpendicular to the reflected plane.

$$\sigma_{xy} = \begin{vmatrix} x_1 \\ y_1 \\ z_1 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{vmatrix} \begin{vmatrix} x \\ y \\ z \end{vmatrix} \tag{2}$$

$$\sigma_{yz} = \begin{vmatrix} x_1 \\ y_1 \\ z_1 \end{vmatrix} = \begin{vmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix} \begin{vmatrix} x \\ y \\ z \end{vmatrix} \tag{3}$$

$$\sigma_{xz} = \begin{vmatrix} x_1 \\ y_1 \\ z_1 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{vmatrix} \begin{vmatrix} x \\ y \\ z \end{vmatrix} \tag{4}$$

In the past, the concept of symmetry operation or geometry method was used to prove the law of the combination of symmetric elements in crystallography. However, the problem of "multiplication" of symmetric elements producing a new symmetric element cannot be accurately expressed. The combination of symmetric elements can be thoroughly explained by the group multiplication principle of group theory Law.

3. Magic Cubic

The denotation of the operation on magic cubic is firstly given. Then by using those denotations, some properties generated from group theory establish. In this part of the article, some important denotations are shown to merge the properties of magic cubic and the properties of group theory.

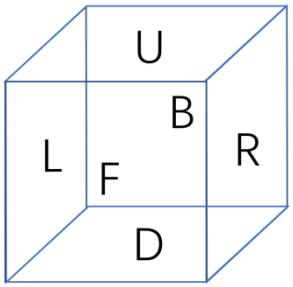

Figure 1. Name of the surfaces

Let the operation of clockwise rotation on magic cubic be denoted as illustrated in Figure 1. Denote U as up surface, D as down surface, F as front surface, B as behind surface, L as left surface, R as right surface respectively.

Let the operation of clockwise rotation on magic cubic be denoted as below:

Denote U^{-1} as up surface, D^{-1} as down surface, F^{-1} as a front surface, B^{-1} as behind surface, L^{-1} as left surface, R^{-1} as right surface respectively [9].

Let X, Y both denote the effects of many rotations to the magic cube and let the operation of XY denote that the magic cube is firstly affected by X and then is affected by Y.

If c represents any state of the magic cube, then it follows that $XY(c) = Y(X(c))$, which means the operation of XY can be viewed as a compound operation of the function.

It can be demonstrated that the set $\langle\{U, D, F, B, L, R\}\rangle$ generated by the operation is a group.

The positions of small color patches and small blocks:

Other denotations should be made to demonstrate the relationship between patches, blocks on the magic cube, and group theory.

Let F_* denote the set of all positions of the small color patch on the magic cube. Then it can be found that $|F_*| = 4 \times 9 = 36$.

Let B_* denote the set of all positions of small blocks on the magic cube. Then $|B_*| = 3^3 - 1 = 26$ since there needs no center block in the magic cube.

Let $P = \{u, d, f, b, l, r\}$ denote the positions of the surface of the magic cube following the initials of words of positions as above (for example, u represents the upper position).

By using the set P, the following symbols can be denoted:

$\forall x, y, z \in P, xyz$ patch is the small color patch on x surface and border on both y, z surface.

$\forall x, y \in P, xy$ patch is the small color patch on x surface and only border on y surface.

$\forall x, y, z \in P, xyz$ block is the small block that has three surfaces on x, y, z surfaces.

$\forall x, y \in P, xy$ block is the small block that has two surfaces on x, y surfaces.

Let us denote the set of all xy patches (edge patches) as E_F, the set of all xyz patches (corner patches) as V_F, the set of all xyz blocks (edge blocks) as E_B, denote the set of all xy blocks (corner blocks) as V_B.

Then G is a group acting on $E_F, V_F, E_B, V_B, F_*, B_*$.

For convenience, U, D, F, B, L, R is also used to represent the function of themself acting on any set in $E_F, V_F, E_B, V_B, F_*, B_*$. The set it is acting on will be mentioned in the article in advance.

The permutations of the rotations acting on F_*, E_F, V_F:

The permutations of patches, blocks, and operations have some interesting connections, which emphasize that it is possible to use mathematics to describe a magic cube. Each operation can be represented as a permutation of patches or blocks.

For the rotations acting on F_*, we have:

(1). $U = (ulb\ ubr\ urf\ ufl)(ub\ ur\ uf\ ul)(bul\ rub\ fur\ luf)(bu\ ru\ fu\ lu)(bru\ rfu\ flu\ lbu)$

(2).$D = (dbl\ dlf\ dfr\ drb)(db\ dl\ df\ dr)(bld\ lfd\ frd\ rbd)(bd\ ld\ fd\ rd)(bdr\ ldb\ fdl\ rdf)$

(3). $F = (flu\ fur\ frd\ fdl)(fu\ ft\ fd\ fl)(ufl\ rfu\ dfr\ lfd)(uf\ rf\ df\ lf)(urf\ rdf\ dlf\ luf)$

(4). $B = (bul\ bld\ bdr\ bru)(bu\ bl\ bd\ br)(ulb\ ldb\ drb\ rub)(ub\ lb\ db\ rb)(ubr\ lbu\ dbl\ rbd)$

(5). $L = (luf\ lfd\ ldb\ lbu)(lu\ lf\ ld\ lb)(ufl\ fdl\ dbl\ bul)(ul\ fl\ dl\ bl)(ulb\ flu\ dlf\ bld)$

(6)$R = (rfu\ rub\ rbd\ rdf)(ru\ rb\ rd\ rf)(urf\ bru\ drb\ frd)(ur\ br\ dr\ fr)(ubr\ bdr\ dfr\ fur)$

The group acting on E_F, V_F, E_B, V_B is transitive, but the group acting on F_*, B_* is not.

For the rotations acting on E_F, the subset $\{xy, yx\}$ is primitive, so the action is imprimitive. Similarly, for the rotations acting on E_F, V_F, the subset $\{xyz, yzx, zxy\}$ is primitive, so the action is imprimitive.

The permutations of the rotations acting on B_*, E_B, V_B: by further implications of concepts of group theory, some important properties of a magic cube can be represented briefly as below.

The commutator in group theory is denoted as $[g,h] = ghg^{-1}h^{-1}$. Some delicate series of rotations that can keep most of the patches unchanged and alter some special ones can be represented by a commutator. For example:

(1). $[U,F]^2 = (uf\ ur\ fl)$

(2). $[U,F]^3 = (ufl\ fdl)(fur\ ubr)$

There are also more complicated commutators including conjugation, such as:

(1). $[F^{-1}RF,L] = (urf\ ufl\ ulb)$

(2). $[B[F,D^{-1}]B^{-1},U^2] = (urf\ ubr)(ufl\ ulb)$

Let S_V denote the set of all permutations of G acting on V_B and S_E denote the set of all permutations of G acting on E_B. Then S_V, S_E are groups. Furtherly, the cross product $S_V \times S_E$ can denote the set of all permutations of G acting on B_*, which is a group.

To differentiate, A acting on V_B, E_B are denoted as A', A'' respectively. Furtherly we can denote $\sigma: G \to S_V$, where $\sigma(g) = g'$ and $\tau: G \to S_E$, where $\tau(g) = g''$. It can be shown that σ, τ are homomorphisms.

The direction of the corner blocks and the edge blocks:

Using patches to represent operations is too lengthy, whereas using blocks to represent operations cannot contain the direction information of each block. So new way should be figured out to represent the direction of every block when the magic cubic is in any state.

The direction of xyz blocks and xy blocks are denoted separately. In each case of xyz blocks or xy blocks, all the blocks are represented in a set, where the pair in the set has two elements. The left element represents which block it is, and the right element represents the direction of the block.

Each xyz block is denoted by numbers, as shown in Figure 2. Each xy block is denoted by numbers, as shown in Figure 3:

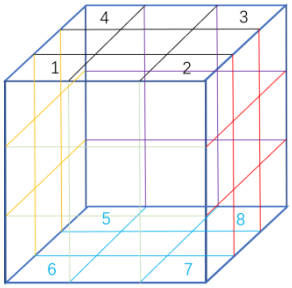

Figure 2. Number of the xyz blocks

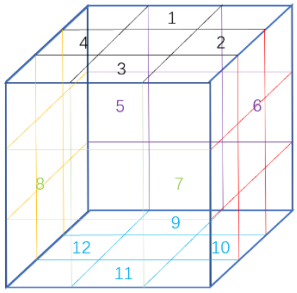

Figure 3. Number of the xy blocks

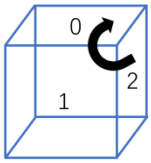

Figure 4. Number on the patch of the directions of the xyz blocks

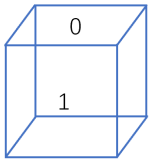

Figure 5. Number on the patch of the directions of the xy blocks

The direction of each block is denoted by the number on the patch, which is on the surface of the block number. In Figure 4,5, originally, zero is on the surface of the block number. For Figure 4, if we rotate the block clockwise, then 1 comes up (down) to the surface of the block number, and after that 2 comes up (down). For Figure 5, if we invert the block upside down, then 1 comes up (down) to the surface of the block number.

The set of possible directions of all corner blocks is denoted as $D_V := \{\{(a, i_a)|a \in \{1,2,\dots,8\}\}|\forall a, i_a \in \{0,1,2\}\}$. And the set of possible directions of all edge blocks as $D_E := \{\{(a, i_a)|a \in \{1,2,\dots,12\}\}|\forall a, i_a \in \{0,1\}\}$. Let $C_V := \{(a,0)|a \in \{1,2,\dots,8\}\}, C_E := \{(a,0)|a \in \{1,2,\dots,12\}\}$, then C_V is the primary state of the direction of corner blocks, C_E is the primary state of direction of edge blocks.

We default that $\forall V \in D_V, \sigma(g)(V) = \left\{v\begin{pmatrix}\sigma(g) & 0\\ 0 & 1\end{pmatrix}|v \in V\right\}$, and $\forall E \in D_E, \tau(g)(E) = \left\{e\begin{pmatrix}\tau(g) & 0\\ 0 & 1\end{pmatrix}|e \in E\right\}$. We also default that $\forall V_1, V_2 \in D_V, V_1 + V_2 := \{(a, i_{a1} + i_{a2})|a \in \{1,2,\dots,8\}\}$, where $(a, i_{a1}) \in V_1$ and $(a, i_{a2}) \in V_2$; $\forall E_1, E_2 \in D_E, E_1 + E_2 := \{(a, i_{a1} + i_{a2})|a \in \{1,2,\dots,12\}\}$, where $(a, i_{a1}) \in E_1$ and $(a, i_{a2}) \in E_2$.

Let $v(g)$ denote the element in D_V which represents the state after rotation g is put into the state C_V. Let $w(g)$ denote the element in D_E which represents the state after rotation g is put into the state C_E.

It can be deduced that:

$$\forall g_1 g_2 \in G, v(g_1 g_2) = v(g_1) + \sigma(g_1^{-1})(v(g_2)) \text{ and } w(g_1 g_2) = w(g_1) + \tau(g_1^{-1})(w(g_2)). \quad (5)$$

Furtherly there are:

$$\begin{aligned}\forall g_1 g_2 \in G, v(g_1 g_2 g_3) &= v(g_1) + \sigma(g_1^{-1})\big(v(g_2 g_3)\big)\\ &= v(g_1) + \sigma(g_1^{-1})\Big(v(g_2) + \sigma(g_2^{-1})\big(v(g_3)\big)\Big)\\ &= v(g_1) + \sigma(g_1^{-1})v(g_2) + \sigma(g_1^{-1}g_2^{-1})\big(v(g_3)\big). \quad (6)\\ \forall g_1 g_2 \in G, w(g_1 g_2 g_3) &= w(g_1) + \sigma(g_1^{-1})\big(w(g_2 g_3)\big)\\ &= w(g_1) + \sigma(g_1^{-1})\Big(w(g_2) + \sigma(g_2^{-1})\big(w(g_3)\big)\Big)\\ &= w(g_1) + \sigma(g_1^{-1})w(g_2) + \sigma(g_1^{-1}g_2^{-1})\big(w(g_3)\big). \quad (7)\end{aligned}$$

4. Commutative Group

Theorem 4.1 *Assume that G is an n order group, and we have known $n-1$ elements, then the n^{th} element is solely determined.*

Proof : The Operation rule of a finite group is shown by the multiplication table [10]. Assume the result of multiplication between $n-1$ elements $x_1, x_2, \dots, x_{n-1}$ in G shown in the table of [10].

As the corresponding line for identity is the same as the first line of the chart in [10], if neither of the lines showing in the chart is the same as the first line, then x_n is the identity. Conversely, if there is an element whose corresponding line is the same as the first line, this means that it is the identity. For convenience, let us assume x_1 is the identity. It is obvious that whilst x_1 is the identity, x_n did not appear in the $a_{1,1}$, $a_{1,2}$, …, $a_{1,n-1}$. Moving to the second line, there must be an element is x_n in $a_{2,1}$, $a_{2,2}$, …, $a_{2,n-1}$, otherwise, $a_{2,n} = x_2 x_n = x_n$, which means x_2 is the identity too, and it is contradictory to the uniqueness of identity. Therefore, there must be an element that shows in $a_{2,1}$, $a_{2,2}$,…, $a_{2,n-1}$, and did not appear in $a_{1,1}$, $a_{1,2}$, …, $a_{1,n-1}$, this element is x_n.

It is worth mentioning that when G is a commutative group, the n^{th} element could be easily determined without using a multiplication table.

Theorem 4.2 *Assume that G is a n order commutative group, n is an odd number. $G = A \cup \{x\}, x \notin A$, then $x = (\prod_{g \in X} g)^{-1}$*

Proof: Consider mapping φ of G: $x \to x^{-1}$. φ is a one-to-one mapping of G, $\varphi(I) = I$, when $x \neq I$, $\varphi(x) \neq x$, if not, $x^{-1} = x$, then $x^2 = I$, and it can be easily derived that $2 \| G|$, which is contradictory to the assumption. Therefore, we can pair the rest of the elements in G, except the identity I, and the product of each group is I. As G is a commutative group, we have $\prod_{g \in G} g = I$, then, $\prod_{g \in A} g = x^{-1}$, then, $x \prod_{g \in A} g = I$, therefore, $x = (\prod_{g \in A} g)^{-1}$.

There must be an element of order 2 in a group of n, when n is an even number. We call this kind of element involution [11].

Theorem 4.3 Assume that G is a n order commutative group, n is an even number, and $G = A \cup B \cup \{x\}$, and A contains every non-involutive element other than x, whilst B contains every involutive element other than x, then $x = g_0(\prod_{g \in A} g)^{-1}$, and g_0 is an involutive element.

Proof: Classify elements in G into two categories: A_0 contains every non-involutive element, B_0 contains every involutive element. In view of Theorem 4.2, the product of every non-involutive element in G is I, $\prod_{g \in A_0} g = I$, and due to the product of every two involution in the commutative group is still an involution, we have $\prod_{g \in B_0} = g_0$, g_0 is one involution; thus, $x \prod_{g \in A \cup B} g = \prod_{g \in A_0} g \prod_{g \in B_0} g = g_0$, therefore, $x = g_0(\prod_{g \in A} g)^{-1}$.

Corollary 4.4 *Assume that $G = \langle a \rangle$ is an n-order cyclic group, and $G = A \cup \{x\}, x \notin A$, then if n is an odd number, $x = (\prod_{g \in A} g)^{-1}$, otherwise, if n is an even number, $x = a^{\frac{n}{2}}(\prod_{g \in A} g)^{-1}$.*

Proof: As $x \prod_{g \in A} g = \prod_{g \in G} g = a^{\sum_{i=1}^{n-1} i} = a^{1+2+\cdots+(n-1)} = a^{\frac{n(n-1)}{2}}$, if n is an odd number, $a^{\frac{n(n-1)}{2}} = a^{n\frac{n-1}{2}} = 1$, if n is an even number $a^{\frac{n(n-1)}{2}} = a^{n\frac{n}{2}} \cdot a^{-\frac{n}{2}} = a^{-\frac{n}{2}} = a^n \cdot a^{-\frac{n}{2}} = a^{\frac{n}{2}}$.

Example 4.1 Assume that there are a set of cards. Each card is one of five colors: red, yellow, purple, blue, and green, with an identifier. The first digit of the identifier is the letters A to Z, and the second and third digits are numbers 00 to 99. Each card has a different identifier, so there are $5 \times 26 \times 100 = 13000$ cards. This set of cards is kept by A and B, respectively (the number of cards does not need to be the same). Now one piece is missing how to find out the characteristics of the lost card (assume that the cards of A and B cannot be put together)?

The finding method is shown as follows:

Step 1.

Use 0,1,2,3,4 for five colors, red, yellow, purple, blue, and green, and represented by group Z_5.

Use 0,1,2，…，25 for letters A to Z, and represented by group Z_{26}.

Use 0,1,2，…，99 for numbers 00,01,02，…，99, and represented by group Z_{100}.

After these works, the color and identifier of each card make a one-to-one map with a commutative group $G = Z_5 \times Z_{26} \times Z_{100}$. Then the characteristic of a lost card maps a lost element in group G.

Step 2.

Take out every card from A, calculating the following number separately:

1) $(1 \times yellowcards + 2 \times purplecards + 3 \times bluecards + 4 \times greencards) \div 5$, record the remainder as a_1.

2) $(1 \times letterB + 2 \times letterC + \cdots + 25 \times letterZ) \div 26$, record the remainder as b_1.

3) $(1 \times number01 + 2 \times number02 + \cdots + 99 \times number99) \div 100$, record the remainder as c_1

c_1.

Take out every card from B, calculating a_2, b_2, c_2 similarly.

Step 3.

Assume $a_1 + a_2 \equiv a(mod\ 5)$, $0 \leq a < 5$, as 5 is an odd number, given Corollary 4.4, the lost element in Z_5 is the inverse of a, which is $5 - a$.

Assume $b_1 + b_2 \equiv b(mod\ 26)$, $0 \leq b < 26$, as 26 is an even number, in view of Corollary 4.4, the lost element in Z_{26} is the inverse of b plus 13, but as each element in Z_{26} has been summed for 5×100 times, there are 500 pieces of 13 in G. Let the sum of them be S_b, $S_b = 6500 \equiv 0(mod\ 26)$, therefore, the lost element in Z_{26} is $26 - b$ as before.

Assume $c_1 + c_2 \equiv c(mod\ 100)$, $0 \leq c < 100$, as 100 is an even number, because of Corollary 4.4, the lost element in Z_{26} is the inverse of c plusing 50, but as each element in Z_{26} has been summed for 5×26 times, there are 130 pieces of 50 in G. Let the sum of them be S_c, $S_c = 6500 \equiv 0(mod\ 100)$. Therefore, the lost element in Z_{100} is $100 - c$ as before.

At last, we have an array $(5 - a, 26 - b, 100 - c)$, which exactly is the characteristic of a lost card. For example, array (3,17,36) represents the blue card R36.

Example 4.2. Assume that there is an eight-number password. To improve privacy, the password is safekeeping by $n(n < 10^8)$ different people, so that any 1，$2,3$，…，$n-1$ people could not figure out the password.

The safekeeping method:

Number 10^8 cards by 00000000 to 99999999, pick out one card randomly and make it the password. Divide the rest of the cards casually into n parts. Each part is kept by a different person. Therefore, any 1，$2,3$，…，$n-1$ people could not figure out the password, but it will be easily figured out by n people, by putting every card together and checking which number is lost, but it will be loads of work to do. We can still figure the password out using the method of Corollary 4.4:

Everyone adds the number of the card kept by themselves, then divided by 10^8, record the reminder as a_i. Assume that $\sum_{i=1}^{n} a_i \equiv a(mod\ 10^8)$,$0 \leq a < 10^8$. In view of Corollary 4.4, the password is the remainder of $\frac{1}{2} \times 10^8 - a$ divided by 10^8, which means, when $a > 5 \times 10^7$, the password is $10^8 + \frac{1}{2} \times 10^8 - a = 15 \times 10^7 - a$, if $a \leq 5 \times 10^7$, the password is $5 \times 10^7 - a$.

In real life, everyone doesn't have to remember every card they keep. The only thing they need to keep is the a_i that we have mentioned before. This way of keeping passwords is safe and efficient. Take 10 people to keep a password as an example, if everyone keeps the same amount of cards (only one person less than others). If k people try to guess the password, the possibility of picking the right password out is $\frac{1}{(10-k)\times 10^7 - 1}$, this number is smaller than 10^7, which means it is likely that they need to guess millions of times to figure out the password.

5. Conclusion

In this paper, two methods of figuring up the last element in a group by using the properties of the group are shown. One is fitting for every n order group. The other makes it easier when a group is a commutative group. At the end of the paper, two examples are given to illustrate how to use these methods to solve practical problems such as finding lost items and password safekeeping. The way it works and why this strategy is safe and efficient are also analyzed. The application of group theory to geometry or other mathematical and physical objects seems obvious, but it is difficult to use general mathematical tools to give an accurate and general description of the concept of symmetry, especially the calculation of the number of symmetric properties.

References

[1] Pesic P 2012 An introduction to tensors and group theory for physicists[J]. Physics Today, vol.65. pp.64.
[2] Robinson D 1996 A course in the theory of groups. Springer-Verlag. Springer-Verlag, New York.
[3] Pain J C 2022 Sum rules for Clebsch–Gordan coefficients from group theory and Runge-Lenz-Pauli vector. Journal of Physics Communications, Vol. 6. pp. 5
[4] Rodriguez-Nieto J G Salazar-Diaz O P and Velásquez R 2022 Sylow-type theorems for generalized groups. Journal of Algebra and its Applications, pp.2350162.
[5] Liu T Hu G K and Dong J Q et al. 2022 Renormalization group theory of eigen microstates. Chinese Physics Letters, Vol.39. pp.8.
[6] Apruzzi F Bhardwaj L and Gould D et al. 2022 2-Group symmetries and their classification in 6d. SciPost Physics, vol.12. pp.098.
[7] Debnath S 2022 Neutrosophic fuzzy soft matrix theory and its application in group decision making. In Handbook of Research on Advances and Applications of Fuzzy Sets and Logic, pp.741-770.
[8] Thomas J I 2022 The principle of mathematical induction: applications in physical optics. Journal of Applied Mathematics.
[9] Zhu L 2008 The Applications of Group Thoery in Rubik's Cube.
[10] Cayley Arthur 1854 VII. On the theory of groups, as depending on the symbolic equation θn= 1. The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science vol.7. pp. 40-47.
[11] Kurzweil H 1997 Endliche Pruppen[M]. Springer-verlag. Berlin-Heidelberg-New York. .